REMARKS

Reconsideration and allowance of the subject patent application are respectfully requested.

The specification has been amended to include headings.

Claims 6-10 were rejected under 35 U.S.C. Section 101 as allegedly being directed to non-statutory subject matter.

Applicant respectfully submits that claims 6-10 fall within the statutory category of patentable subject matter under 35 U.S.C. Section 101 of a machine. Specifically, these claims as amended define a "system" comprising, among other things, a compiler analyser, an instruction frequency analyser, and a frequency distribution checker. These elements are defined as being operative to perform particular functions, and so are clearly directed to a system. As described by way of example and without limitation in the subject patent application, these elements may be part of a virus scanning engine for e-mails processed by a mail gateway at an ISP. See, e.g., page 4, lines 11-18. As set forth in Annex II of the "Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility," the Supreme Court has defined a machine as "a concrete thing, consisting of parts or of certain devices and combinations of devices." *Burr v. Duryee*, 68 U.S. (1 Wall) 531, 570 (1863). Applicant submits that claims 6-10 define such a machine, as being directed to a system such as a computer system. To further emphasize this, claim 6 has been amended to refer to a "computer" system.

The office action contends that the claims are an example of "functional descriptive material." Applicant disagrees. The features of a compiler analyser, an instruction frequency analyser, and a frequency distribution checker are operative to perform particular functions. Thus, the claims properly define elements of a machine, not descriptive material.

Withdrawal of the Section 101 rejection of claims 6-10 is respectfully requested.

Claims 1-10 were rejected under 35 U.S.C. Section 103(a) as allegedly being made "obvious" by Nachenberg (U.S. Patent No. 6,357,008) in view of Kephart et al. (U.S. Patent No. 5,675,711). While not acquiescing in this rejection or in the characterizations of the applied documents in the office action, independent claims 1 and 6 have been amended. Conforming amendments have been made to the dependent claims as appropriate. The discussion below makes reference to the amended claims.

In claim 1, the program file is described as "comprising program code" to provide antecedent basis for the steps of identifying the compiler and determining the frequency distribution by reference to that program code. Moreover, the step of identifying a compiler involves identifying a compiler "from a set of predetermined compilers." An additional feature of "maintaining a database holding frequency distributions of machine code instructions or sequences thereof expected for respective compilers in the set of predetermined compilers" is also introduced, and the comparison in step d) is described as being with "the frequency distribution of machine code instructions or sequences thereof stored in the database as being expected for the compiler identified by the

compiler analyser." By way of example and without limitation, these amendments find support in the description and use of database 80 at page 4, lines 1-10 and page 4, lines 30-33. This description makes clear that the virus detection in the illustrative embodiments is based on comparison with frequency distributions (of machine code instructions or sequences thereof) which are specific to the compiler used to create the program code.

The office action contends that Nachenberg discloses all the features of claim 1 except for the feature of identifying the compiler used to create the program code, but that it would have been obvious to provide Nachenberg with this feature based on the disclosure of Kephart et al. Applicant respectfully submits that this rejection is not applicable to the amended claims, although this is without any admission or agreement that the rejection is correct with respect to the original claims. Indeed, some parts of the rejection with respect to the original claims are traversed below.

Claim 1 recites *a database holding frequency distributions of machine code instructions or sequences thereof expected for respective compilers in the set of predetermined compilers*. The comparison of the frequency distribution determined from the file being scanned is *with the frequency distribution of machine code instructions or sequences thereof stored in the database as being expected for the compiler identified in step a)*. Thus, claim 1 recites that the comparison of the frequency distribution determined from the file being scanned is with a frequency distribution stored in the

database which is dependent on the identified compiler. This is the expected frequency distribution for the compiler stored in the database.

The claim 1 method involves this interrelationship between the identified compiler and the frequency distribution of machine code instructions or sequences thereof used in the comparison. As discussed by way of example with reference to the illustrative embodiments at page 4, lines 1-10 of the subject patent application, (1) virus code will have been created by a compiler that is in general different from the compiler used to create the program into which the virus code is inserted, and (2) consequently, a comparison of the actual frequency distribution of machine code instructions with the frequency distribution expected for the actually identified compiler is indicative of the presence or absence of a virus. Specific deficiencies of the proposed combination of Nachenberg and Kephart et al. will be discussed in greater detail below, but, in general terms, neither of these documents provides any disclosure or suggestion of the comparison recited in claim 1.

The office action alleges that step b) of claim 1 (step c) in original claim 1) is disclosed in Nachenberg at col. 16, lines 50-65. This passage of Nachenberg discloses observing "various suspicious operations" or "behaviours" and counting the occurrences thereof. This relies on the "various suspicious operations" or "behaviours" meeting the requirement of the "machine code instructions" recited in claim 1. Applicant strongly traverses any such alleged correspondence because the "various suspicious operations" or

"behaviours" in Nachenberg are the effect of the program, not machine code instructions, as is clear from the examples at col. 16, line 64 to col. 17, line 11.

Nachenberg is further deficient for the following reasons.

Nachenberg does not disclose the step of identifying the compiler and this is acknowledged in the office action. See 10/10/2007 Office Action, page 3.

Moreover, Nachenberg does not disclose maintaining a database as set forth in step c) of claim 1. Specifically, this step recites that frequency distributions are held "for respective compilers in the set of predetermined compilers." Even assuming (for purposes of discussion only) that the "various suspicious operations" or "behaviours" of Nachenberg are erroneously viewed as corresponding to the claimed machine code instructions, the same set of suspicious operations or behaviors is always observed.

Further, step d) recites that the comparison is with "the frequency distribution of machine code instructions or sequences thereof stored in the database as being expected for the compiler identified in step a)." This specifies that the comparison is with one of the frequency distributions in the database, depending on the compiler identified in step a). Clearly this is not disclosed or suggested by Nachenberg, who does not identify a compiler at all.

In short, Nachenberg lacks any disclosure or suggestion of identifying the compiler and basing a comparison thereof.

Kephart et al. does not remedy the deficiencies of Nachenberg.

Kephart et al. relates to a classifier for classifying data strings. The main application of the classifier disclosed in Kephart et al. is to detect viruses in the data strings. The office action references col. 2, lines 1-15 and col. 4, lines 55-63 of Kephart et al. These passages relate to a different application of the classifier from virus detection. In particular, they disclose application of the classifier to identify the compiler used to generate the software under analysis. Kephart et al. states that this is useful in the field of reverse engineering of software (see col. 2, lines 1-2). Furthermore, Kephart et al. states that one reason why knowledge of this compiler is useful is to obtain source code from machine code for the purpose of analyzing a virus (col. 2, lines 6-12).

Even assuming for the sake of argument that Kephart et al. is viewed as disclosing identifying a compiler, Kephart et al. does not disclose the features of step c) and d). That is, there is no disclosure in Kephart et al. of storing or using frequency distributions of machine code instructions or sequences thereof expected for respective compilers which may be identified. Thus, there is no disclosure of step c) of maintaining a database holding frequency distributions of machine code instructions or sequences thereof expected for respective compilers which may be identified. Similarly, there is no disclosure of the feature of step d) of the frequency distributions of machine code instructions or sequences thereof expected for the identified compiler being used as the basis for a comparison to detect a virus.

The office action alleges that one of ordinary skill would be motivated to combine the identifying of a compiler disclosed in Kephart et al. with Nachenberg. Applicant does

not agree with this contention, but even if it is notionally accepted for the sake of argument, this does not render the claim 1 method obvious because of the above-noted deficiencies of Kephart et al.

The basis for virus detection in Nachenberg is observing "various suspicious operations" or "behaviors" and counting the occurrences thereof. There is nothing in Kephart et al. which teaches or suggests modifying this basis of virus detection in dependence on the identified compiler, as required by step d).

As pointed out in the office action, Kephart et al. discloses that identification of the compiler is useful for the purpose of decompiling a machine code virus to allow analysis of the source code. However, Kephart et al. does not go beyond this and does not provide the claimed features as set forth above. In particular, Kephart et al. does not teach that a comparison of the actual frequency distribution of machine code instructions with the frequency distribution expected for the actually identified compiler is indicative of the presence or absence of a virus. Consequently, claim 1 is not made obvious by the proposed combination of Nachenberg and Kephart et al.

Claim 6 recites analogous features to those present in claim 1 and consequently this claim patentably distinguishes from the proposed Nachenberg-Kephart et al. combination for the reasons discussed above.

Claims 2-5 depend from claim 1 and 7-10 depend from claim 6. These claims patentably distinguish from the applied documents because of their respective dependencies and because of the additional patentable features recited therein.

New claims 11-14 have been added. The subject matter of these new claims finds support in the original disclosure and the Examiner is invited to independently confirm that this is the case.

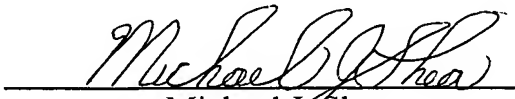
Claims 11 and 12 depend from claims 4 and 9, respectively, and patentably distinguish from the applied documents at least because of these dependencies.

Claim 13 recites a computer readable medium having stored thereon instructions for causing a computer to carry out a method for scanning a computer file containing program code for virus infections. The method is like that of claim 1 and therefore claim 13 is believed to patentably distinguish over the applied documents. Claim 14 refers to claim 13.

The pending claims are believed to patentably distinguish over the applied documents and favorable office action is respectfully requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 
Michael J. Shea
Reg. No. 34,725

MJS:mjs
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100